Okano-Heijmans, Maaike; Vosse, Wilhelm M.

Article

Promoting open and inclusive connectivity: The case for digital development cooperation

Research in Globalization

Provided in Cooperation with:
Elsevier

Suggested Citation: Okano-Heijmans, Maaike; Vosse, Wilhelm M. (2021) : Promoting open and inclusive connectivity: The case for digital development cooperation, Research in Globalization, ISSN 2590-051X, Elsevier, Amsterdam, Vol. 3, pp. 1-10, https://doi.org/10.1016/j.resglo.2021.100061

This Version is available at:
https://hdl.handle.net/10419/330993

Research in Globalization 3 (2021) 100061

Contents lists available at ScienceDirect

Research in Globalization

journal homepage: www.sciencedirect.com/journal/research-in-globalization

Promoting open and inclusive connectivity: The case for digital development cooperation

Maaike Okano-Heijmans [a,*], Wilhelm Vosse [b,*]

[a] The Netherlands Institute of International Relations 'Clingendael', The Hague, Netherlands
[b] International Christian University (ICU), Tokyo, Japan

ARTICLE INFO

Keywords:
Digital development cooperation
European Union
Indo-Pacific
Connectivity

ABSTRACT

A focus on digital development cooperation as a cornerstone in Europe's digital connectivity agenda offers opportunities to act on long-term challenges and addresses several key priorities identified by the European Commission in third countries. This article develops an argument for strengthening Europe's agenda on digital development cooperation, specifically in the Indo-Pacific region. After first conceptualizing digital development cooperation, we argue that the key reasons for the EU to step up its digital development efforts in the Indo-Pacific region are the societal impact of disruptive technologies; the power shift towards the Indo-Pacific; the expanding clout of the Chinese Digital Silk Road; and the implications of the US-China tech conflict. The EU's 2030 Digital Compass provides an ideal framework to envision the digital development cooperation initiatives of European and Asian players. The EU can benefit from cooperation and coordination with like-minded partners in the Indo-Pacific.

1. Introduction

A focus on digital development cooperation as a cornerstone in Europe's digital connectivity agenda offers opportunities to act on long-term challenges and addresses several key priorities identified by the European Commission and its member states in third countries (European Parliament Members' Research Service, 2020). Digital development cooperation is important for both developmental and normative reasons, as it helps countries to reap the benefits from the digital transition - for example by facilitating broadband access, introducing digital tools to reap higher yields from agricultural land or to improve governance, and providing access to bank accounts that will support access to finance for the poor as well as women in business. Set against a context of rising digital authoritarianism, this will also contribute to the spread of liberal norms like openness, transparency and privacy in the digital domain.

Digital cooperation efforts by the EU and its member states are largely shaped by three, partly overlapping domains: the connectivity agenda, the digital agenda, and the regional agenda - in our case, for the Indo-Pacific. Future EU action on digital development cooperation will depend on a coordinated approach by policymakers and stakeholders working in these fields. This requires a proper understanding of evolving policies in these three fields and a joined-up approach of relevant institutions, which until now have largely been discussed and acted separately. Our article may be understood as an attempt to clarify the interlinkages between the three agendas. Also, it develops an argument for strengthening Europe's agenda on digital development cooperation, specifically in the Indo-Pacific region.

After first conceptualizing digital development cooperation, we argue that the key reasons for the EU to step up its digital development efforts in the Indo-Pacific region are the societal impact of disruptive technologies; the power shift towards the Indo-Pacific; the expanding clout of the Chinese Digital Silk Road; and the implications of the US-China tech conflict. Next, we discuss Europe's tilt towards the Indo-Pacific since 2020. Building on these insights, the final section analyses the digital development cooperation activities and future agenda of the EU and its member states as well as Asian countries along the frame provided in the 2030 Digital Compass published in March 2021. In this document, the Commission sets out the direction of 'Europe's Digital Decade.' The four core objectives are the furthering of (1) digitally skilled citizens and highly skilled digital professionals; (2) to secure performant and sustainable digital infrastructures; (3) the digital

* Corresponding authors at: Professor of Politics and International Relations and Chair of the Department of Politics and International Studies, International Christian University (ICU), Osawa 3-10-2, Mitaka City, Tokyo 181-8585, Japan (W. Vosse). Senior Research Fellow at The Netherlands Institute of International Relations 'Clingendael' and Visiting Lecturer at the University of Leiden (M. Okano-Heijmans).
E-mail addresses: mokano-heijmans@clingendael.org (M. Okano-Heijmans), vosse@icu.ac.jp (W. Vosse).

https://doi.org/10.1016/j.resglo.2021.100061
Received 16 April 2021; Received in revised form 24 July 2021; Accepted 23 August 2021
Available online 30 August 2021

transformation of businesses; and (4) the digitalisation of public services (European Commission, 2021a).

Our analysis suggests that the EU can benefit from cooperation and coordination with like-minded partners in the Indo-Pacific. We argue that all four dimensions of Europe's Digital Compass must also be considered in (relation to) third countries, especially developing countries and emerging economies in the Indo-Pacific; which is not the case today. That is moving beyond the bilateral context of connectivity partnerships, like that between the EU and Japan and the EU and India, and acting in a region where growth, security and stability is a key interest of the EU and its member states as well. Europe's long-term stability depends on a more international strategy to defend Europe's interests in the digital age. A focus on digital connectivity, and digital development cooperation as a key element of this agenda, will be instrumental to this.

Empirical evidence and examples for existing and the potential for future projects will be from one region in particular, namely the Indo-Pacific region where China's presence has been most substantial and where the stakes for Europe are thus rising. China is a relatively newer player but also the country that invests most funds in the digital domain. At the same time, countries like Australia, Japan, South Korea, Taiwan, and Singapore have been setting up capacity-building projects to improve cybersecurity and government and business digital infrastructure, security, and norms in ASEAN member states. For comparison purposes, we at times consider selected examples of European initiatives in Africa, which can be seen as models for a more active stance in developing countries in the Indo-Pacific.

2. What is digital development cooperation?

In essence, digital development cooperation[1] entails efforts to help developing countries and emerging economies to reap the benefits and address challenges of the digital transformation that developed countries go through as well. Although it is certainly not a new phenomenon and not the only tool used for this objective, scholarly and practical thinking about digital development cooperation needs to reflect on the current challenges and opportunities. This involves examination and reevaluation of the subject in its proper geopolitical context - that is, set against shifting global power balances and a hardening US-China tech-data conflict, and the accompanying battle for norms and standards in the digital domain. Clearly, digital development cooperation is rising in importance, but the concept itself has not yet received sufficient recognition in the academic and policy debate and have not yet led to a mainstreaming of the digital dimension in development policy and practice, in the same way, green development cooperation has normalized ecological and environmental considerations in development projects. It should be considered hand in hand with other instruments, such as trade promotion efforts that help develop business-to-business relations to stimulate local digital economies.

Digital development cooperation thus goes beyond the grants and loans for traditional ICT-projects, which have been in place for decades, and technical training on the ground or in the donor country. It includes assistance with the design and implementation of infrastructural broadband projects, as well as capacity building with the aim of governance of the digital domain that reflect norms and values of a free and open internet (Pawlak & Barmpaliou, 2017; Global Forum on Cyber Expertize (GFCE), 2021; World Bank Group, 2019).

[1] In an earlier paper (Okano-Heijmans & Vosse, 2020) we used the concept "digital ODA," however, reflecting on comments from some reviewers that ODA is a concept defined by the OECD as grants, loans and technical assistance, we now use the term 'digital development cooperation' as a broader concept that includes public–private partnerships, the activities of non-governmental organizations, and the activities such as technical assistance and norm-setting. See also Table 1.

Digital development cooperation involves each of digital connectivity's three strands – namely (a) telecommunications infrastructure, (b) regulation and (c) business – and has both practical and strategic objectives.

In the regulatory field, the digital development cooperation-agenda primarily involves digital capacity building – that is, assisting third countries on how to establish data protection structures and prevent cybercrime, and cross-border e-commerce and data transfer rules. This includes training, scholarships and dialogues to exchange information and best practices. In doing so, the EU can also promote an inclusive, human-centred ICT environment that emphasizes transparency, openness and privacy of users in the digital domain. The General Data Protection Act (GDPR) is by now recognized by many third countries as a 'golden standard' that can inspire national legislation elsewhere, and the EU can draw inspiration from this success to strengthen dialogues with third countries on other regulation (that is partly still in the making), such as for trustworthy Artificial Intelligence (AI Regulation), and of digital markets (the Digital Markets Act, balancing innovation and fairness), digital services (the Digital Services Act, to protect freedom of speech online), and data (the Data Governance Act, seeking to establish a digital identity that puts users in control).

Digital development cooperation in the business-dimension could help to ensure that these countries can keep the control over their own data for their domestic business development, rather than allowing foreign companies to gather local data and use it for their own benefit. Digital financial inclusion and a focus on fintech can also contribute to such private-sector development.

Finally, on the telecommunications infrastructure side, digital development cooperation can play a role in helping to design and secure telecommunication and data infrastructure. After all, as per the EU Connectivity Strategy, 'high capacity network links are critical to support the digital economy (…and…) universal and affordable access to the internet is a proven enabler of socio-economic development.' Importantly, digital development cooperation is not an appropriate tool to promote the actual building of certain telecommunications infrastructures, which is contracted from governments to companies. Next to concessional loans that help finance broadband infrastructure projects, as part of development cooperation efforts, investment promotion and investment financing instruments (economic diplomacy) are needed to promote the adoption by other countries of trusted and secure telecommunications hardware. A key point to note is that the digital development cooperation agenda needs to be considered in connection with other instruments that promote Europe's digital interests in this field.

Table 1 is an attempt to highlight the difference between our concept of digital development cooperation and established concepts like capacity building, development assistance or cooperation, and the World Bank's development partnership as a response to UN SDG target 9.c, aiming for a significant increase in access to ICT and universal and affordable access to the Internet in least developed countries.

Digital development cooperation received a significant push with the creation in December 2018 of the European Union-African Union Digital Economy Task Force (EU-AU DETF), a multi-stakeholder platform that includes the private sector, donors, international organisations, financial institutions and civil society. The task force published a report in June 2019 relaying a shared vision, a set of common agreed principles and a list of policy recommendations and actions focusing on four main objectives. There is a remarkable overlap between the EU-AU DETF report and the 2030 Digital Compass. They share the same key objectives, namely (1) access to affordable broadband connectivity and digital infrastructure; (2) the development of digital skills; (3) support for digital entrepreneurship; and (4) development and support for e-services: e-government, smart cities, e-commerce and eHealth (European Commission, 2020).

Another instrumental push towards greater EU action on digital development cooperation came in December 2020 with the report of the

Table 1
Distinguishing aspects of digital development cooperation.

	Digital Development cooperation	Cyber Capacity Building	OECD Development Assistance/ Cooperation	World Bank Digital Development Partnership / UN SDG 9c
Instruments				
Cyber capacity building	YES	YES	Limited	
Technical Assistance/ Training	YES	YES	Limited	
ICT Infrastructure Development	YES	–	YES	
Loans for expanding ICT network	YES	–	YES	YES
Grants for expanding ICT network	YES	–	YES	YES
Public-private partnerships	YES	YES	Limited	YES
New objectives				
B2B in ICT	YES		Limited	
Privacy Protection	YES	Limited	–	
Protection against cyber attacks	YES	YES	–	
Free and open internet	YES	YES	–	
Preventing dominance of a few companies	YES	–	–	
Digital Divide	YES	–	YES	YES

European Parliament (EP) prepared by EP Member Reinhard Bütikofer (Bütikofer, 2020). The report calls on the European Commission and the EEAS to bring the EU Connectivity Strategy to a global level. Amongst many other things, it recommends that the Commission identifies real needs for targeted digital development cooperation and strengthen partnerships with democracies around the world that share our fundamental values.

We argue that success in digital development cooperation requires that these first steps and intentional documents have to be followed by concrete activities and projects by the EU and its member states. We would secondly argue that while projects on the African continent and in the European neighbourhood - where most EU development efforts focus today - should be continued, Europe also needs to turn its focus to the Indo-Pacific region. So far, the combined share of EU development assistance to Asia was less than 13%. India with a of 300 million Euros is the only country in the top-10 recipients of EU gross bilateral ODA[2].

Digital development cooperation requires that it is properly budgeted, staffed and coordinated, which is not the case today. Also, programmes need to target more than the traditional developing countries[3]. Finally, digital development cooperation stands to benefit from better coordination and best practice learning between various players. This article aims to contribute to this latter point.

3. Why digital development cooperation in the Indo-Pacific?

As digital technologies profoundly reshape societies, countries risk being left behind in the fourth industrial revolution and becoming a playground of US-China rivalry. This leaves the EU and its member states – with partners – with a role and responsibility to show that there are alternatives, beyond what China and the US propose. Digital development cooperation can contribute to securing liberal norms like openness and transparency, rather than allowing an all too strong state or dependence on giant tech companies. After all, long-term support of third countries' governments can only be achieved through persuasion, and not force. Four key reasons to invest in digital development cooperation, in particular in the Indo-Pacific, are thus: (1) rapid technological development and its impact on society; (2) the power shift towards the Indo-Pacific; (3) concerns related to China's Digital Silk Road; and (4) the US-China tech-data conflict. This section discusses these factors in more detail.

3.1. Disruptive technologies

Disruptive technologies are fundamentally changing the world we live in. While they provide great opportunities for innovation and economic development, the use of information technology more broadly, and of cyberspace in particular, is undermining democratic values in democratic countries and weakening real or potential opposition in authoritarian states (see for example Barrinha & Renard, 2020). The last decades have seen a decline of countries that can be considered fully free or where the majority of the public unconditionally supports democratic values and the free and open exchange of a wide range of opinions and lifestyles. Media freedom, for example, is under threat in an increasing number of countries and governments are less accountable and tolerant to different ideas than they were just ten years ago. Information and communication technology (ICT) has played a major role in undermining or weakening liberal and democratic values in recent years, such as some countries in Eastern Europe and the Western Balkans (Freedom House, 2020). Other studies have shown a similarly worrisome influence of Chinese information infrastructure and surveillance technology in countries in the Indo-Pacific region (Nouwens & Lons, 2021; Mochinaga, 2020; LY and Tan, 2020).

As many countries in the Indo-Pacific region have weak democratic and civil traditions on the one hand, and are still in the early developmental stages on the other, they are more prone to succumb to authoritarian leadership styles, constraining civil and political rights. At the same time, European countries, and most countries in the Indo-Pacific, suffer from the weakness that many of the most powerful tech companies are either US or Chinese owned. Importantly, this also positions US and Chinese companies as global standard-setters, including for the gathering, monitoring and use of data, thereby also giving their governments a strategic advantage. The fact that Europe and like-minded countries in the Indo-Pacific also have a different vision of the use of these advanced technologies, is an incentive for closer cooperation on developing their own, or protecting their data and eventually the survival of their respective economic, political and socio-cultural visions.

3.2. Economic and power shift towards the Indo-Pacific

Over the last two decades, we have witnessed a tectonic power shift from major Western economies and political players who ruled the world for the last century towards the Indo-Pacific potentially under the leadership of China. The share of GDP (PPP) that is produced in the Indo-Pacific region has reached 62% of world GDP in 2020, while the EU share has shrunk to just 15%, and is predicted to shrink even further over

[2] See: OECD (2021), Aid at a glance charts, at: https://www.oecd.org/dac/financing-sustainable-development/development-finance-data/aid-at-a-glance.htm

[3] This seems to be the case with the Neighbourhood, Development and International Cooperation Instrument (NDICI) instrument) which aims to spend almost €30 billion on Sub-Saharan Africa and €8.5 billion in Asia and the Pacific countries (as per the EU's connectivity strategy). See: (European Commission, 2021b).

the next decade. China is already the major extra-EU trading partner for most European countries as well as most countries in the Indo-Pacific.

The Indo-Pacific is home to three out of the four largest economies outside the EU (China, Japan and India) and by 2030, 90 percent of 2.4 billion new middle income class members will come from the Indo-Pacific region. Stability in the Indo-Pacific is crucial for the stable and secure supply of critical goods, which depends on open maritime and trade routes. In addition, countries in the region are key players to tackling global challenges, such as climate change, pandemics and poverty reduction. This also goes for a properly functioning international legal order.

As detailed in section four, by March 2021, the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Josep Borrell had started to act on the fact that the "shift in the world's centre of gravity to the Indo-Pacific started years ago" and that the EU needed "to look at the consequences in geopolitical and geo-economic terms." The EU and the member states are thus now redefining their approach to the Indo-Pacific, in which the EU Connectivity strategy would need to play a central role (Borrell, 2021). An EU Strategy for Cooperation in the Indo-Pacific was announced in the EU Council Conclusions of April 2021, with a comprehensive Joint Communication of the EU High Representative and the European Commission expected to follow in September 2021 (Council of the European Union, 2021a).

3.3. China's Digital Silk Road

China is a key player in digital connectivity in the Indo-Pacific and beyond. Its Digital Silk Road (DSR), part of the broader Belt and Road Initiative, aims at promoting and facilitating the digital economy, including cross-border e-commerce and digital payment systems, in developing countries and emerging economies (Majcherczyk & Shuqiang, 2019). DSR contributes to ICT infrastructure that provides access to the internet and aims to establish an inter-regional credit guarantee mechanism to cope with the complexities of the online trading environment. Chinese ICT infrastructure investment was until 2017 relatively small compared to other sectors like transportation, construction and energy, accounting for 29.3%, 22.6% and 20.0% of total projects respectively, compared to 2.7% for the ICT sector (Gong et al., 2019, p. 4–5).

Chinese activities under the DSR are increasingly also seen as a threat to the so-called free and open internet. Since the early 2010s, the influence of the Chinese IT sector has vastly grown, especially in the area of 5G infrastructure technology and companies like Huawei or ZTE. Huawei has a global market share of 28 percent and ZTE one of 10 percent in 5G equipment. With its "Made in China" strategy, China aims at becoming the global technological leader for a whole range of future technologies, from telecommunications, AI infrastructure, 3D printing, online payment systems to online cultural exchange (e.g. WeChat) to digital governance, data management and cybersecurity.

Developing countries in the Indo-Pacific region with weak democratic and civil traditions are an ideal target for Chinese ICT infrastructure investment, which provides their governments with control and surveillance instruments. In turn, these instruments can be used to strengthen their hold of power while giving Chinese companies (and as an extension, the state) a potential backdoor to their data. Europe shares the concern for a global shift towards a less liberal or post-liberal world order with like-minded countries in the Indo-Pacific and beyond, facilitated in large part by the growing power and influence of social media and information and communications technology more broadly.

China has also been actively involved in capacity building in Africa as well as in ASEAN countries. For example in 2013, it hosted the First Workshop of the ASEAN Regional Forum (ARF) on cybersecurity (Homburger, 2019, p. 235). China is also actively engaging in partnerships with the Shanghai Cooperation Organization to shape their cyber norms through establishing their Code of Conduct. Zine Homburger (2019) discussed the feasibility of cyber capacity building for the debate on international norms in cyberspace. Her results indicate that the evidence for a direct effect is rather weak, but is worried that rather leading to norm cohesion, it might lead to norm fragmentation. Important in the context of the main argument of this paper, she also stresses that cyber capacity building alone will not necessarily lead to changes in cyber norms. So, while recognizing the added value for countries that seek to reap the benefits of the digital era, there is little doubt that Chinese ICT has also been a factor in further weakening civic and political norms and practice in a number of countries in the Indo-Pacific region. This includes providing authoritarian leaning countries with surveillance technology that will further tighten the state's hold on power in countries such as Cambodia, Myanmar, Pakistan and the Philippines - but also beyond the Indo-Pacific: Saudi Arabia, Egypt, and Zimbabwe (Kyodo News, 2019; Harsono, 2020; Murgia & Yang, 2019) and inspiring other countries, including Cambodia, to establish a China-style internet firewall (AFP, 2021). Freedom House stresses that China sells surveillance technology such as face recognition cameras made by Huawei as in the "Safe City Agreement" with 10 of the 29 countries categorized as "nations in transit" (NIT) from democratic to authoritarian systems. While Chinese influence is not exclusive to these countries but is increasingly also recognized by Western European countries as a potential threat to them, the fact that the EU and many of its member states have been actively engaged to help democratize these countries and provided political and economic assistance also because of their geographic proximity, has increasingly become a concern for Europe (Freedom House, 2020; Dekker et al., 2020).

3.4. The US-China tech conflict

A final geo-strategic reason why European actors have and will need to become more active in Africa as well as the Indo-Pacific region is the ongoing so-called US-China tech conflict. The strategic competition between the US and China that initially focused on tensions in the South China Sea has contributed to rising antagonisms and a larger great power military presence. In recent years, this competition has also intensified economic and technological rivalry that is further heightening tensions in the region. A key element herein is standard-setting: technological and market standards that shape the competitiveness of companies, as well as governance norms, where democracies increasingly compete with digitally empowered authoritarian states. For example, the secure and ethical use of smart city applications and data by authorities must be ensured, lest they contribute to far-going digital surveillance by states.

The deepening US-China tech war is triggering a decoupling between a free and open cyberspace in large parts of the Western world, and a closed or semi-closed cyberspace in China and its sphere of influence. In addition to a decoupling on the software and data side comes a potential decoupling of hardware and ICT equipment. The era of globalization with global supply chains which we have seen prosper and grow especially since the early post-Cold War period might come to an end. Under president Xi, China has begun a plan towards economic and technological self-reliance, while an increasing number of Western countries including most of Europe have abandoned Chinese 5G equipment and communications technology and limited market access of Chinese social media companies such as Tiktok (Inkster, 2021; Inkster, 2020; Zeng et al., 2017).

This is catapulting the EU and its member states in a strategic position as a balancing power, seeking to protect their own interests and to avoid - and helping others to avoid - being forced into a binary choice between the great powers and to maintain their ability to act autonomously. In other words, it is in the EU's own interest to present an alternative to what China and the US are offering, especially as divergences arise with the latter on digital governance and economic policies. Polls among elites in Southeast Asia show that the EU is also welcomed in such a role, as the number of people who believe that the

EU will 'do the right thing' to contribute to global peace, security, prosperity and governance' have grown in 2020 from already high levels (Seah et al., 2021).

4. Europe's role in the Indo-Pacific

For most European countries, the Asian region has not traditionally been a focus of attention of their foreign or development policy. European countries which used to have colonies in the Indo-Pacific region, namely the United Kingdom and France, or countries like Portugal and the Netherlands that have long historical and security relationships have long been the exception. However, over the last decades, economic relations between Europe and countries like Japan, Korea, and China, and to a lesser degree also some countries in Southeast Asia have deepened. Today, the EU is the biggest investor in the ASEAN countries and until 2020 was the biggest trading partner of the region, is second only to Japan as ASEAN's most favoured and trusted strategic partner in the hedging game against US-China rivalry (Seah et al., 2021).

China is now the main trading partner outside of the EU of most European countries. Given that China's economy is still growing, export-oriented countries like Germany, the UK and the Netherlands traditionally have a strong interest in keeping smooth trading relations with China. In recent years, however, they have developed a more complete picture of China - not just as an economic partner, but also as a country with a different political system with a reach beyond its own borders, and whose approaches do not always align with the more liberal, transparent and human-centered ideals of Europe. This has led to a strategic reassessment of China in Brussels - outlined in the 2019 EU-China Strategic Outlook (European Commission, 2019) - and of many EU member states.

While a more critical stance in bilateral relations with China is one side of the coin, deeper cooperation with other countries that share EU concerns with regard to China may be considered the other side of that same coin. Steps towards an EU Indo-Pacific approach fall into that latter category: a push for more comprehensive and assertive indirect China policy that seeks to balance and restrain – but not to constrain – China's growing role and influence in the region as well as on the multilateral stage. After all, a concert of powers in the Indo-Pacific is also in Europe's interests, as the EU's economic growth, political and military stability is closely intertwined with that of the region.

Thus, the EU is embarking on its own distinctive strategic approach to the Indo-Pacific region, following steps in this direction by most of its strategic partners in Asia - specifically, Japan, the United States, India and ASEAN. Since the Indo-Pacific as a term has its roots in the maritime domain, it is hardly surprising that countries in the region have so far primarily called for greater maritime presence by the EU and specific member states. While it is indeed important that the EU promotes maritime security, unhindered safe passage on shipping routes and maritime governance, European actors have an interest in thinking beyond the maritime realm as they consider actionable steps. Digital connectivity is important, as China currently dominates the digital economy in the Indo-Pacific and has been active in exporting its brand of 'digital authoritarianism' through programmes like the Digital Silk Road. Thus, the EU should look to contribute to open, safe and inclusive digital connectivity and engage with the thriving digital economies in the Indo-Pacific to ensure democratic standards are upheld.

To varying degrees, the Indo-Pacific documents of France, Germany and the Netherlands (that pushed the EU debate) and the EU Indo-Pacific Strategy (that followed) recognize the challenges and the importance of action in the digital and cyber domains. Digital development cooperation is not explicitly mentioned. After briefly outlining the relevant core strategic concerns of the EU and its member states here, examples of existing and possible future digital development cooperation initiatives that support cybersecurity and the digital transformation are introduced in more detail in the *Analysis: Digital development cooperation in the Indo-Pacific* below.

France was the first EU member state to develop an Indo-Pacific Strategy, already starting in 2018. Since 2019, the French government has been developing strategic partnerships with India, Australia, Japan, Malaysia, Singapore, New Zealand, Indonesia and Vietnam and has been working with the ADMM + and its "Plus" Partner countries for decades, because it wants to actively contribute to the regional security order in the Indo-Pacific (Ministry of Defense of France, 2019). Because of its post-colonial ties to the region with sizable French permanent residents who need to be protected, close cooperation with military forces in the region, France considers itself an Indo-Pacific power. (Ministry of Defense of France, 2019, p. 5). While France's first Indo-Pacific paper was published by the Ministry of Defense, its broader interests were articulated in the French Indo-Pacific Strategy (Ministry for Europe and Foreign Affairs, 2019) and finally by the President on behalf of the French government (Government of France, 2021). Herein, 'economy, connectivity and research and innovation' are recognized as one of four pillars, and specific mention is made of the importance of standards and cyber security.

Germany's Indo-Pacific policy guidelines stresses shifting of economic and political power towards the Indo-Pacific region (Ministry of Foreign Affairs of Germany, 2020, p. 2). Germany is particularly concerned about a shift to a new bipolar global structure, led by the United States and China, and equally the hegemonic influence of China in the Indo-Pacific region (p. 3–4), and prefers a united European approach towards the Indo-Pacific, based on strengthening multilateralism, a rules-based order. Germany sees "digital transformation and connectivity" as one of the core areas where Europe needs to provide leadership. It is concerned about an impending split of the so far global internet, and the setting of new standards and norms, which could further weaken the influence of European markets but also values and norms in the world. Therefore, one of these areas where Germany suggests closer cooperation is in cybersecurity and digital connectivity (p. 4, 8.)

Third in line, the Netherlands has also put their stake on the ground with their Indo-Pacific Guidelines of November 2020. It sees a strong need for itself and for the EU to step up their efforts in the Indo-Pacific and develop a distinctive Dutch and EU vision of the region. Also, the Guidelines call for an intensification of bilateral cooperation with like-minded countries in the region that share support for democratic values, the rule of law, human rights, and a transparent and sustainable market economy. The digital and cyber domain emerges, next to the maritime domain, as one of one of two focus areas of the Dutch government. The mention in the Dutch Guidelines of courses on building cyber capacity in ASEAN countries in areas including international law in the digital domain - although not new - is perhaps the only example of digital development cooperation in any of the European documents on the Indo-Pacific (Government of the Netherlands, 2020b).

At the instigation of the French, German and Dutch governments, debates about EU action in the Indo-Pacific were starting to be held also in EU-context from September 2021. In January 2021, Japanese Foreign Minister Toshimitsu Motegi addressed the European Union's Foreign Affairs Council on the topic. An EU Strategy for Cooperation in the Indo-Pacific was subsequently announced in the EU Council Conclusions of April 2021, with a comprehensive Joint Communication of the EU High Representative and the European Commission expected to follow in September 2021. The inclusive European strategy sets out to deepen cooperation, in particular with like-minded partners, across a broad range of priority areas, including research and development (R&D) cooperation and connectivity (Council of the European Union, 2021a).

Summing up, the turn of the EU and its member states to the Indo-Pacific stems from a concern that the Indo-Pacific region is becoming the playground of major powers, which would limit the options of countries in the region and limit the potential influence of Europe. Therefore, Europe has to reach out to new partners to provide them with real strategic options, rather than having to choose between the U.S. and the Chinese model. Digital development cooperation could be one

important instrument to this objective.

5. Analysis: Digital development cooperation in the Indo-Pacific

Overall, efforts of the EU and its member states in digital development cooperation now focus on developing countries in Africa and the European neighbourhood. Thematically, they mainly address digital inclusion and enhanced digital resilience, thereby enabling specific groups to take advantage of the digital revolution (see for example Government of the Netherlands, 2020a; Digital 4 Development Hub, 2021; European Digital Development Alliance, 2021). Digital infrastructure, which is the backbone of digitalization and the e-economy, remains a basic need in many African and Indo-Pacific countries but is a blind spot in the agenda of European countries. China, by contrast, has been responding to this need in the developing world. This is important for European countries, as e-economies that are largely built on Chinese infrastructure will complicate European digital development cooperation efforts that seek to compel African and Asian governments to make digital inclusion central to their future development trajectories.

The following paragraphs discuss the digital development cooperation activities and future agenda of the EU and relevant member states as well as key Asian players along the frame provided in the 2030 Digital Compass. As stated earlier, this Compass focuses on four fields, namely digital skills, digital infrastructures; the digital transformation of businesses and of public services (European Commission, 2021a).

5.1. Digitally skilled citizens and highly skilled digital professionals

A few countries in the Indo-Pacific region, most notably Japan, Singapore, South Korea, India and Taiwan have started projects and initiatives with the aim to increase the number of digitally skilled citizens and the quality of training for digital professionals. The EU and several EU member states' efforts in this field have been rather scant.

Japan's core focus in digital development has long been on improving the cyber capacity of less mature countries with a strong focus on Southeast Asia. Japan's National Center of Incident Readiness and Strategy for Cybersecurity aims at (1) sharing its expertise and coordination of policies, (2) assist in incident response, and (3) capacity building, and encourages Japanese companies and other stakeholders to contribute to the security of cyberspace and the security environment in other countries. Japan's latest success is the opening of the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) in Bangkok in September 2018. Its core objective is the improvement of skills of security-related agencies in ten ASEAN countries and the development of a standardized Incident Reporting Framework across the region by establishing an ASEAN-CERT.

Singapore is undoubtedly one of the most active players in cybersecurity and cyber capacity building in Southeast Asia and for ASEAN members in particular. In 2016, Singapore brought telecommunications and other relevant ministers together for the first ASEAN Ministerial Conference on Cybersecurity (AMCC), aiming at (1) tighter regional cybersecurity cooperation and (2) the use of digital technologies for economic progress and improvement of living standards across the region. To make such cooperation more permanent and enable practical and technical cooperation, Singapore suggested the establishment of an ASEAN Cyber Capacity Program (ACCP) to help ASEAN nations to improve their IT infrastructure to counter cyber threats, through cyber capacity-building and confidence-building measures. One result is the opening of the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) in Singapore in October 2019.

South Korea's digital development cooperation is active in Asia and Africa. In Asia, Korea's Overseas Infrastructure Development Support Corporation (KIND) supports Korean companies to advance into the new southern region's infrastructure development projects through continuous monitoring and support - bilaterally and through the ASEAN Global Infrastructure Fund. It also aims at improving the 5G networks in ASEAN countries and India through the 2019 5G + Strategy for the realisation of innovation and growth initiative. In Africa, Korea cooperates in multiple bilateral and multilateral initiatives on cyber issues.

India's potential for digital development cooperation stems largely from its domestic experience with the use of digital tools to spur development. India had remarkable successes with efforts to enhance digital financial inclusion through digital payment systems. The question now is whether this success can be exported to other developing countries, either by India as a development player of its own or in a trilateral format, with European partners. Trilateral cooperation with Indian companies with a proven track record could facilitate improved access to countries, particularly in Africa. Cooperation may be sought with India's Centre for Digital Financial Inclusion (CDFI), which promotes the use of technology to support its welfare programs and financial mainstream for the poor, with a valuable track record on digitizing benefit delivery from, implementing data-driven frameworks from governance and to farm services; and promoting basic financial literacy using digital communication tools. For now, it operates within India, however, its experiences could be of benefit to individuals in many other developing countries.[4]

In recent years, the European Union and some of its member states have also begun to establish their own cyber capacity building projects in the Indo-Pacific region, and at the same time established or deepend joint projects with partners such as Japan or Singapore. Examples are the "Cybersecurity Awareness and Knowledge Systemic High-level Application" (YAKSHA) project which ran from 2018 to 2020 and aimed at building partnerships in the cybersecurity domain with ASEAN countries by developing a solution tailored to specific users and national needs[5].

While these are important steps in the right direction, there is still a gap between expectations from Asian countries, what the EU is able to do in the region, and the types and levels of assistance and cooperation the EU and its member states have provided so far. Chen and Gao (2020), for example, recognize the deepening of EU-Asia ties in nontraditional security including cybersecurity and the broadening of EU-ASEAN, ARF, and ASEM cyber capacity building initiatives and instruments (as mentioned above), but they also highlight an effectiveness and expectation gap. They criticize among others the often low degree of cohesiveness of EU security policy towards Asia and its over-ambitious objectives, which can weaken how serious the EU is being taken by Asian countries.

5.2. Secure, performant and sustainable digital infrastructures

Several European and Indo-Pacific countries have been active in a number of projects with the aim to secure performant and sustainable digital infrastructures. The focus here is on fostering sustainable and secure digital infrastructures, and regulation and governance that respects norms of openness, decentralization, privacy and transparency that benefit the whole society.

The EU has so far widely neglected the basic element of building hard infrastructure. This is problematic, as it fails to recognize that digital societies and e-economies that are largely built on Chinese infrastructure will complicate development cooperation efforts that seek to compel Asian governments to make digital inclusion central to their future development trajectories.

[4] See the CDRI website:http://www.cdfi.in/ and author's interview with CDRI director Krishnan Dharmarajan on 17 January 2020, Bangalore.

[5] The project was funded under the European Union's Horizon 2020 research and innovation programme and reinforced European Union (EU) and Association of SouthEast Asian Nations (ASEAN). See details of the Yaksha Project here: https://project-yaksha.eu/project

5.2.1. Internet governance and digital regulation

Like the EU, Japan has a strong incentive in norm-setting and internet governance such as the United Nations Group of Governmental Experts (UNGGE) and the United Nations Open-Ended Working Group (OEWG). Japan is specifically concerned about the undermining of the free and open internet by some countries (esp. China and Russia), and, therefore, has started a range of initiatives in less cyber mature countries in Southeast Asia for strengthening an understanding, awareness and support for an open and free internet and the rule of law in cyberspace. The EU and Japan also agree that "existing international law, including the Charter of the United Nations, applies to cyberspace" and both actively contribute to "discussions on the individual and specific applications of existing international law and the development and universalization of norms." (National Center of Incident Readiness and Strategy for Cybersecurity (NISC), 2018).

Japan and Europe both favor a multi-stakeholder approach in Internet governance, which had been used and was and is a successful approach in global and regional governance, since the 2015 stalemate at the United Nations Group of Governmental Experts (UNGGE) and the attempt of Russia and China and to some degree India to set up and alternative more government focused Open Ended Working Group, global internet governance has become more difficult for Japan and the EU. Therefore, the EU and Japan use the EU-Japan cyber security dialogue and other fora to coordinate their approach and motions in these international governing bodies. As the success of this approach in defending a free and open internet to protect democratic and anti-authoritarian values heavily depends on convincing the large number of state actors in the Indo-Pacific region that this is also in their interest, the EU-Japan policy framework towards the Indo-Pacific already has, but needs to further emphasize and push for these values. They both need to make the point that peace and prosperity in the Indo-Pacific is heavily dependent on an open and transparent internet governance which needs to include a broad range of political and social (non-state) actors from within and outside their respective countries.

Among EU member states, Germany's concrete cooperation initiatives in the Indo-Pacific aim at expanding cyber-security cooperation to protect information and communications systems and collective defence capabilities with partners with shared values such as Singapore, Australia, Japan and South Korea. Germany is increasingly concerned that certain actors are trying to undermine rules-based digital networks by pushing through rules and regulations which benefit certain state actors (e.g. internet surveillance, privacy).

France has also been actively involved in deepening scientific and technological opportunities and highlights lack or shortage of regulations and subsequently the risk that cyberspace and advances in satellite technology are likely to exacerbate rivalries between states in the Indo-Pacific (Ministry of Defense of France, 2019, p. 5). For this reason, France is one of the most active European players in science diplomacy in the Indo-Pacific region, where it has set up dozens of research partnerships and outposts of the French research and development agency (Ministry for Europe and Foreign Affairs, 2019).

The Dutch Indo-Pacific Guidelines highlights new security threats such as cyber espionage and cyber attacks, for example on the finance and banking infrastructure in the region. The Netherlands has already begun to work with Singapore to improve cyber capacity building in ASEAN countries. They are a strong supporter of the EU digital sustainable connectivity (Digital Strategy), which also reflects a concern about potential misuse or dominance by some states of artificial intelligence, data privacy, and in the end the so-called digital sovereignty of countries in the Indo-Pacific.

5.2.2. Digital infrastructure: The foundation of the digital economy and society

Digital inclusion and enhanced digital resilience can only be achieved with the availability of that hard infrastructure, which remains a basic need in rural areas of many Indo-Pacific countries. Telecommunications networks are the backbone of digitalization, while phones and data packages can bring more citizens online. This agenda remains a weak spot in the European agendas, also when considering a wider variety of instruments beyond digital development cooperation specifically. An exception that should also inspire EU action in the Indo-Pacific, is the involvement of the European Investment Bank (EIB) in improving the telecom infrastructure and connectivity in Africa through the EU-Africa Infrastructure Trust Fund. Between 2015 and 2020 it sponsored projects worth about €120 million, such as the expansion of telecom infrastructure in Kenya, the construction of solar-powered mobile towers in Sub-Saharan Africa especially the DRC, and the expanding high-speed internet access in cities across Angola.

The South Korean New Southern Policy does include a stronger 'hard infrastructure' element. It aims at strengthening relations with new southern countries (ASEAN and India) to achieve co-prosperity of the Korean Peninsula and Southeast Asia. Part of this policy is the 2019 5G + *Strategy for the realisation of innovation and growth* initiative, which seeks to further cooperation between 5G mobile communication, K-smart (Smart City, Smart Factory, Smart Farm), and Korea Start-up Centre are in progress between South Korea, ASEAN countries and India. During the special summit in 2019, bilateral agreements on economic cooperation were reached between South Korea and several ASEAN countries. On smart cities, this involves sharing of know-how with Singapore, and cooperation with Vietnam and Brunei, on science and technology cooperation with Thailand, and ICT cooperation with Malaysia and Brunei.

For its part, China has been responding to the basic need for hard infrastructure in the developing world, providing the donor countries with the necessary digital infrastructure. While China's digital silk road initiative has spent almost $80 billion in projects around the world and billions on African digital and telecommunications infrastructure, data centers and so-called smart cities since its inception in 2015, a lot of it is in the form of direct Chinese telecom company investments and another in market-level loans, which has led to debt crises in many countries in Africa (Prasso, 2019). The most severe problem for Africa and a chance for Europe is that China has already used the Chinese-build IT infrastructure to spy on governments and international institutions in Africa, and accusations of an "authoritarian future for the internet" if China is in control of core IT infrastructure (CyberLaw (2018), Rahn (2019)).

The EU has also begun a number of projects in cooperation with countries in Asia as well as in Africa. Some D4D projects intend to improve cybersecurity norms and regulations[6]. The Global Action on Cybercrime Extended (GLACY)+ (Council of Europe, 2020a) aims at strengthening legal and policing institutions to combat cybercrime and is jointly funded by the European Union and the Council of Europe and implemented by the latter. While the geographic focus of GLACY (2013–2016) and GLACY+ (2016–2024) is more on African countries, it does include projects in the Philippines and Sri Lanka. One reason why it has so far not been extended to more countries in the Indo-Pacific is that it aims at assisting signatories of the Budapest Convention on Cybercrime (Council of Europe, 2001) to implement policing of cybercrime and cybercrime legislation, and as of July 2021, only two Indo-Pacific

[6] Examples are Cyber4Dev (2018 and 2021), a project to promote cyber-resilience and cybersecurity in cooperation with the British, Dutch, and Estonian governments, with projects in Vietnam, Thailand, Sri Lanka, Laos, Cambodia and the Philippines, as well as in Kenya, the DRC, Rwanda and Mauritius. Other African projects are the West African Response on Cybersecurity and Fight Against Cybercrime (OCWAR–C) (European External Action Service (EEAS), 2019) aims at enhancing security and combat cyber-crime in the ECOWAS region, and two joint EU and the Council of Europe projects CyberSouth (Council of Europe, 2020b) in Northern Africa.

developing countries, namely the Philippines and Sri Lanka, have signed the Budapest Convention[7]. The European Union and the CoE should make stronger efforts to encourage more countries in the Indo-Pacific to sign the Budapest Convention, as cybercrime is certainly an area where both Europe and countries in the Indo-Pacific can benefit most, as we can see in Africa[8].

The EU and its member states need to act more assertively and become more active in submitting proposals in internet governance bodies such as the ITU that align with the EU's digital strategy. This is a crucial step to further a democratic decision-making process rather than a process that is dominated by a few large players. European proposals can offer an alternative to the Chinese proposals – as well as the current internet design, which largely benefits US Big Tech – and illustrate the appeal of the 'third way' of Europe that emphasises a so-called 'human-centered approach' to regulation (e.g. of data and artificial intelligence) that promotes openness, inclusiveness and transparency, and includes a strong focus on ethics[9].

First steps in this direction are already being made, by way of the Next Generation Internet (NGI) initiative, which is dedicated to 'fostering a vibrant Open Internet movement that links research, policy and society for the benefit of society.' The EU could take this initiative to the Indo-Pacific and stands to benefit from further cooperation with like-minded countries such as South Korea, Japan and Singapore, whose support will be needed to succeed with implementing this vision to reshape the internet.

5.3. Digital transformation of businesses

The EU has already begun to cooperate with India on certain aspects of the digital transformation of business, especially fin tech. India's potential for digital development cooperation stems largely from its domestic experience with the use of digital tools to spur development. This includes efforts to enhance digital financial inclusion – including through the use of digital payment systems – which achieved remarkable successes in various Indian states. The question now is whether this success can be exported abroad.

This provides an opportunity for European digital development cooperation that could embark on exporting hard and soft digital FinTech infrastructures to the Indo-Pacific region, including through trilateral digital cooperation with India. In doing so, the EU can promote its human-centred approach to the digital domain. The rise and expansion of FinTech in the Indo-Pacific region is fundamentally driven by a large significant share of the population which is unbanked but requires financial services. Internet connectivity is rising, but considerable gaps still exist between urban and rural areas (International Telecommunication Union (ITU), 2020). Potential exists to adapt and export the range of India's FinTech and related public digital platforms. Countries across the Indo-Pacific Asia that are experiencing similar challenges can draw insights from the India Stack story and apply it to address policy gaps.

Beyond FinTech, trilateral digital development cooperation by European countries in the Indo-Pacific region could be expanded to other public goods and services, and partner countries. Singapore and Japan, for example, are active on cybersecurity and cyber capacity-building, while e-health has been a focus area for Taiwan in South-East Asia since before the COVID-19 pandemic (Okano-Heijmans & Vosse, 2020; Hoeksma, 2019). Improved synergies between partners that share European concerns about creeping digital authoritarianism in the Indo-Pacific is needed in order to make the most of the relatively limited funds and action that each actor can bring to the region. Coordinated action and synergies will also contribute to more convergence *vis-à-vis* standards, given the various projects (Dekker et al., 2021).

5.4. Digitalisation of public services

There are several examples for digital development cooperation to enhance the digitalization of public services in the Indo-Pacific region. For example, Taiwanese efforts to improve digital connectivity abroad focus on e-governance, capacity building by sharing experiences in coding and enhancing policy abilities, and jointly developing ICT solutions towards development in a diversity of areas such as healthcare and agriculture. Taiwan's DIGI + is largely domestic, aiming to advance Taiwan as a model for smart tech innovation, but has long favored collaborating with the private sector in third countries, and some elements of this are also taken abroad (Ministry of Foreign Affairs of the Republic of China (Taiwan), 2009; Government of Taiwan International Cooperation and Development Fund, 2010). One specific project carried out by the Taiwanese government is the Taiwan Digital Opportunity Center (TDOC). As part of the New Southbound Policy, the TDOC focuses on improving countries' ICT capabilities and reducing digital divides in the region (Ministry of Foreign Affairs of the Republic of China (Taiwan), 2016).

While Taiwan is by many seen as a frontrunner in the field of digital governance, the EU and some member states have begun to implement certain aspects of e-government that can function as a model for other countries by way of digital development cooperation. For example, several EU member states have developed secure digital identities for all citizens, residents and businesses; in the Netherlands, Digi-D, which allows citizens to identify themselves when making arrangements with governmental, health care or educational institutions over the internet[10]. Building on this, the EU in 2021 proposed a framework for a European digital identity that will allow citizens to access online services with their national digital identification, which will be recognised throughout Europe (European Commission, 2021c). Certainly, the high level of security as well as convenience when dealing with national administrations will be appealing to foreign governments.

The EU activities in digitalization of public services have so far mostly remained in the area of capacity building of public servants for example through EU-ASEAN workshops on cybercrime legislation. Direct investment in ASEAN or more broadly Indo-Pacific digital government infrastructure projects have remained relatively limited. Some in the region have argued that compared to major regional actors like China or the global actors like the United States, apart from the recognition as a norm entrepreneur exemplified in the growing influence of the GDPR, the image of the EU in Asia might not be that of an influential cyber power and a technological leader (Gao & Chen, 2020). Sustainable digital connectivity provides an ideal platform for Europe to increase its IT infrastructure investment in the Indo-Pacific[11].

6. Conclusion

As the EU and its member states embark on their own distinctive approach to the Indo-Pacific, they should seek to contribute to open, safe and inclusive digital connectivity and thriving digital economies in the region. Here, as in Europe's own neighbourhood, the aim should be to establish mutually beneficial relationships on a broad array of digitalization issues.

[7] In addition, Japan, Australia, and New Zealand are also signatories. For the list of signatories, see: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?module=signatures-by-treaty&treatynum=185.

[8] See also the Policy and Regulation Initiative for Digital Africa (PRIDA) with the African Union aims at harmonising the legal and regulatory framework for the use of ICT for social and economic development in Africa.

[9] This European approach contrasts with China's approach that prioritises state security, and with the US approach that prioritises the interests of business. See for example: (Dekker & Okano-Heijmans, 2020).

[10] Examples are filing tax returns or scheduling Covid-tests.

[11] The ASEM Sustainable Connectivity Portal seems to be an ideal model to broaden investment with a European face.

For now, the EU's action in the Indo-Pacific is still catching up with its rhetoric. Even as bilateral connectivity partnerships are being established and the EU's own connectivity strategy is taken global, the EU's action needs to be strengthened in the digital field (Council of the European Union, 2021b). The objectives spelled out in the 2030 Digital Compass offer an excellent framework also for Europe's digital efforts abroad – by way of digital development cooperation. But the Digital for Development (D4D) strategy has lagged both in budget and staff, even if new funds may be expected to come available through the new development cooperation instrument (NDICI). Finally, the forthcoming comprehensive strategy towards Africa and the strategy for cooperation in Indo-Pacific provide a general course for action, but not yet actionable points for digital development cooperation (European Commission, 2020). The focus of the EU and its member states' digital cooperation efforts has so far mainly been on cyber security and digital inclusion.

The EU would do well to also take this broad agenda to the Indo-Pacific. In this region, trilateral digital development cooperation of European countries for example with India in the field of digital financial inclusion could be implemented, and expanded to other public goods and services and partner countries. Singapore and Japan are active on cybersecurity and cyber capacity building, while e-health has been a focus area of Taiwan in Southeast Asia since before the Covid-19 pandemic. Digital development cooperation should also be considered in relation to other instruments (such as investment financing and investment promotion) that can help support the building of hard infrastructure, which also need to be strengthened.

Improved synergies between partners that share European concerns about creeping digital authoritarianism in the Indo-Pacific is needed to make the most of the relatively limited funds and action that each actor can bring to the region. The EU's D4D initiative and similar digital development cooperation programmes of EU member states should also turn to the Indo-Pacific.

CRediT authorship contribution statement

Maaike Okano-Heijmans: Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing - review & editing. **Wilhelm Vosse:** Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing - review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

AFP. (2021). Cambodia sets up China-style internet firewall. Bangkok Post. https://www.bangkokpost.com/world/2069847/cambodia-sets-up-china-style-internet-firewall.

Barrinha, A., & Renard, T. (2020). Power and diplomacy in the post-liberal cyberspace. International Affairs. https://doi.org/10.1093/ia/iiz274.

Borrell, J. (2021). The EU needs a strategic approach for the Indo-Pacific. In EEAS - European External Action Service - European Commission. https://eeas.europa.eu/headquarters/headquarters-homepage/94898/eu-needs-strategic-approach-indo-pacific_en.

Bütikofer, R. (2020). Report on connectivity and EU-Asia relations (2020/2115(INI)) (No. A9-0269/2020). https://www.europarl.europa.eu/doceo/document/A-9-2020-0269_EN.pdf.

Chen, X., & Gao, X. (2020). Bridging the Capability? An Analysis of the New Dynamics in the EU's Security Strategy Towards Asia. *Asia-Pacific Journal of EU Studies, 18*(3), 9–36.

Council of Europe. (2020a). Global Action on Cybercrime Extended (GLACY+). Council of Europe. https://rm.coe.int/3148-glacy-summary-v5/16809c8ad6.

Council of Europe. (2020b). CyberSouth Cooperation on cybercrime in the Southern Neighbourhood Region. https://rm.coe.int/3692-cybersouth-v12-extension/16809e1284.

Council of Europe. (2001). Convention on Cybercrime. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

Council of the European Union. (2021a). EU Strategy for cooperation in the Indo-Pacific [Council Conclusions]. https://data.consilium.europa.eu/doc/document/ST-7914-2021-INIT/en/pdf.

Council of the European Union. (2021b). A Globally Connected Europe (Council {{Conclusions}} No. 10629/21). Council of the European Union. https://data.consilium.europa.eu/doc/document/ST-10629-2021-INIT/en/pdf.

CyberLaw. (2018). African Union headquarters hack (2018) - International cyber law: Interactive toolkit. https://cyberlaw.ccdcoe.org/wiki/African_Union_headquarters_hack_(2018).

Dekker, B., Nachiappan, K., & Okano-Heijmans, M. (2021). Fostering digital connectivity in and with the Indo-Pacific. Clingendael. Netherlands Institute of International Relations. https://www.clingendael.org/sites/default/files/2021-04/Report_Digital_Connectivity_IndoPacific_April_2021.pdf.

Dekker, B., & Okano-Heijmans, M. (2020). *Europe's Digital Decade? Navigating the global battle for digital supremacy*. Clingendael: Netherlands Institute of International Relations.

Dekker, B., Okano-Heijmans, M., & Zhang, E. S. (2020). Unpacking China's Digital Silk Road. Clingendael. Netherlands Institute of International Relations.

Digital 4 Development Hub. (2021). Digital 4 Development. https://d4dlaunch.eu/#about.

European Commission. (2019). EU-China (Joint {{Communication}} to the {{European Parliament}}, the {{European Council}} and the {{Council}} JOIN(2019) 5 final). European Commission. https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf.

European Commission. (2021a). Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_983.

European Commission. (2021b). European Commission welcomes the endorsement of the new billion NDICI-Global Europe instrument to support EU's external action [Press {{Release}}]. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1267.

European Commission. (2021c). Commission proposes a trusted and secure Digital Identity (Text Press Release). https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663.

European Commission. (2020). Towards a comprehensive Strategy with Africa (Joint {{Communication}} to the {{European Parliament}} and the {{Council}} JOIN (2020) 4 final). https://ec.europa.eu/international-partnerships/system/files/communication-eu-africa-strategy-join-2020-4-final_en.pdf.

European Digital Development Alliance. (2021). EDDA - European Digital Development Alliance [Portal]. https://europeandigital.org/.

European External Action Service (EEAS). (2019). West African Response on Cybersecurity and Fight Against Cybercrime (OCWAR C) (p. 2). https://eeas.europa.eu/headquarters/headquarters-homepage/56223/west-african-response-cybersecurity-and-fight-against-cybercrime-ocwar-%E2%80%93-c_en.

European Parliament Members' Research Service. (2020). The von der Leyen Commission's priorities for 2019-2024 (PE 646.148).

Freedom House. (2020). Nations in Transition: Dropping the Democratic Facade. https://freedomhouse.org/sites/default/files/2020-04/05062020_FH_NIT2020_vfinal.pdf.

Gao, X., & Chen, X. (2020). *July). Bridging the Gap: How Can the EU's Digital Connectivity Strategy Fit into East Asia's Digital Landscape.* Closing the Gap.

Global Forum on Cyber Expertize (GFCE). (2021). The Global Cyber Capacity Building Research Agenda 2021. Global Forum on Cyber Expertize (GFCE). https://openarchivaris.nl/blob/51/3e/aa9e67673662d90044c14af58d0f.pdf.

Gong, S., Gu, J., & Teng, F. (2019). The Impact of the Belt and Road Initiative Investment in Digital Connectivity and Information and Communication Technologies on Achieving the SDGs (p. 17) [{{K4D Emerging Issues Report}}]. Institute of Development Studies.

Government of France. (2021). La stratégie de la France dans l'Indopacifique [France's strategy in the Indo-Pacific]. https://www.elysee.fr/admin/upload/default/0001/10/c3852600ccbecbccb2fa05ecf147fa307a79ac17.pdf.

Government of Taiwan International Cooperation and Development Fund. (2010). Themes. In Themes. https://www.icdf.org.tw/ct.asp?xItem=5265&CtNode=29856&mp=2.

Government of the Netherlands. (2020a). Vaststelling begroting Buitenlandse Handel en Ontwikkelingssamenwerking 2021 [{Ontwerpbegroting}]. https://www.rijksbegroting.nl/2021/voorbereiding/begroting,kst282806_5.html.

Government of the Netherlands. (2020b). Indo-Pacific: Guidelines for strengthening Dutch and EU cooperation with partners in Asia (AVT/BZ-201002-011A). https://www.government.nl/documents/publications/2020/11/13/indo-pacific-guidelines.

Harsono, H. (2020). China's Surveillance Technology Is Keeping Tabs on Populations Around the World. The Diplomat. https://thediplomat.com/2020/06/chinas-surveillance-technology-is-keeping-tabs-on-populations-around-the-world/.

Hoeksma, J. (2019). Taiwan targets digital health and smart tech for exports. In Digital Health. https://www.digitalhealth.net/2019/08/taiwan-targets-digital-health-and-smart-tech-for-exports/.

Homburger, Z. (2019). The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace. *Global Society, 33*(2), 224–242. https://doi.org/10.1080/13600826.2019.1569502.

Inkster, N. (2021). *The great decoupling: China.* America and the struggle for technological supremacy: Hurst Publishers.

Inkster, N. (2020). Xi steers China towards economic and technological self-reliance. In IISS. https://www.iiss.org/blogs/analysis/2020/11/china-economic-technological-self-reliance.

International Telecommunication Union (ITU). (2020). Household Internet access in urban areas twice as high as in rural areas [Press {{Release}}]. https://www.itu.int:443/en/mediacentre/Pages/pr27-2020-facts-figures-urban-areas-higher-internet-access-than-rural.aspx.

Kyodo News. (2019). China exports AI surveillance tech to over 60 countries: report. Nikkei Asia. https://asia.nikkei.com/Business/China-tech/China-exports-AI-surveillance-tech-to-over-60-countries-report.

Ly, B., & Tan, A. W. K. (2020). Challenge and perspective for Digital Silk Road. *Cogent Business & Management, 7*(1), 1804180. https://doi.org/10.1080/23311975.2020.1804180.

Majcherczyk, M., & Shuqiang, B. (2019). Digital Silk Road - The Role of Cross-Border E-Commerce in Facilitating Trade. Journal of WTO and China, 9(2), 106–128. https://heinonline.org/HOL/Page?handle=hein.journals/jwtoch9&id=234&div=&collection=.

Ministry of Defense of France. (2019). France and Security in the Indo Pacific. https://www.defense.gouv.fr/layout/set/print/content/download/532754/9176250/version/3/file/France+and+Security+in+the+Indo-Pacific+-+2019.pdf.

Ministry for Europe and Foreign Affairs. (2019). *The French Strategy in the Indo-Pacific*. Government of France. https://www.diplomatie.gouv.fr/en/country-files/asia-and-oceania/the-indo-pacific-region-a-priority-for-france/.

Ministry of Foreign Affairs of Germany. (2020). Policy guidelines for the Indo-Pacific region; Germany Europe Asia: Shaping the 21st century together. https://rangun.diplo.de/blob/2380824/a27b62057f2d2675ce2bbfc5be01099a/policy-guidelines-summary-data.pdf.

Ministry of Foreign Affairs of the Republic of China (Taiwan). (2009). White Paper on Foreign Aid Policy: Progressive Partnerships and Sustainable Development.

Ministry of Foreign Affairs of the Republic of China (Taiwan). (2016). Taiwan Digital Opportunity Center (TDOC) Project. In New Southbound Policy Portal. https://nspp.mofa.gov.tw/nsppe/news.php?post=104415.

Mochinaga, D. (2020). The Expansion of China's Digital Silk Road and Japan's Response. *Asia Policy, 27*(1), 41–60. https://doi.org/10.1353/asp.2020.0005.

Murgia, M., & Yang, Y. (2019). Facial recognition: How China cornered the surveillance market. https://www.ft.com/content/6f1a8f48-1813-11ea-9ee4-11f260415385.

National Center of Incident Readiness and Strategy for Cybersecurity (NISC). (2018). Cybersecurity Strategy. National center of Incident readiness and Strategy for Cybersecurity (NISC). https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf.

Nouwens, M., & Lons, C. (2021). *China's Digital Silk Road: Integration into national IT infrastructure and wider implications for Western defence industries* [Research {{Paper}}]. *The International Institute for Strategic Studies (IISS)*.

Okano-Heijmans, M., & Vosse, W. (2020). Digital connectivity going global: The case for digital ODA. Clingendael Policy Brief. https://www.clingendael.org/publication/digital-connectivity-going-global.

Pawlak, P., & Barmpaliou, P.-N. (2017). Politics of cybersecurity capacity building: conundrum and opportunity. *Journal of Cyber Policy, 2*(1), 123–144. https://doi.org/10.1080/23738871.2017.1294610.

Prasso, S. (2019). China's Digital Silk Road Is Looking More Like an Iron Curtain. Bloomberg.com. https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain.

Rahn, W. (2019). Will China's 5G 'digital Silk Road' lead to an authoritarian future for the internet? | DW | 26.04.2019. In DW.COM. https://www.dw.com/en/will-chinas-5g-digital-silk-road-lead-to-an-authoritarian-future-for-the-internet/a-48497082.

Seah, S., Ha, H. T., Martinus, M., & Thao, P. T. P. (2021). The State of Southeast Asia: 2021 Survey Report. ISEAS-Yusof Ishak Institute. https://www.iseas.edu.sg/wp-content/uploads/2021/01/The-State-of-SEA-2021-v2.pdf.

World Bank Group. (2019). Global Cybersecurity Capacity Program. https://documents1.worldbank.org/curated/en/947551561459590661/pdf/Global-Cybersecurity-Capacity-Program-Lessons-Learned-and-Recommendations-towards-Strengthening-the-Program.pdf.

Zeng, J., Stevens, T., & Chen, Y. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty'. *Politics & Policy, 45*(3), 432–464. https://doi.org/10.1111/polp.2017.45.issue-310.1111/polp.12202.